S-3119

Copy No 2

DF-38

TOP SECRET

The Enigma

by Dr. Rudolf Kochendoerffer

In the following will be given a description of the Enigma, then a case will be described where one succeeded in deciphering a message enciphered by the Enigma and determining the wiring of the machine. In describing the Enigma use will be made of the concept of substitutions and an attempt made to present this concept to non-mathematicians, for what is said about substitutions and their composition might be of use in other decipherments, especially in treating other machines.

I. Description of the Enigma

1. The cipher wheels

The cipher wheels constitute the chief part of the Enigma and are constructed as follows: on each side of a round disc of insulating material are arranged in a circle 26 contacts; on one side there are metal discs, on the other side metal spring contact pins. Each contact on one side is connected by wiring through the disc with a contact on the other side. The choice of the contacts to be connected is termed the wiring (schaltung) of the wheel. To designate the wiring the contacts of the two rings of contacts are assigned numbers 1 - 26 (progressing clockwise when one looks at the side with the spring contacts), contacts standing opposite each other having the same number. The wiring may then be expressed as follows:

$$W = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \\ 11 & 21 & 4 & 3 & 15 & 19 & 13 & 20 & 6 & 10 & 18 & 12 & 1 & 9 & 24 & 14 & 26 & 2 & 16 & 5 & 23 & 25 & 8 & 22 & 17 & 7 \end{pmatrix}$$

In the upper line are the numbers of the contact pins, in the lower those of the flush contacts paired with them. Pin 1 is here connected to flush contact 11, pin 2 with flush contact 21, ... pin 26 with flush contact 7. We treat W, as usual, as a substitution, i.e. as an operation which replaces number 1 by number 11, 2 by 21, etc.

TOP SECRET

2. The wiring of a sequence of two wheels

Fig. 1 shows in schematic form two wheels A and B which are so mounted that the pins of wheel B contact the like numbered flush contacts of wheel A. These wheels have 6 rather than 26 contacts; for simplicity we shall use 6 rather than 26 contacts in our examples since everything essential will be revealed as well. The substitutions produced by the two wheels are

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 2 & 4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 6 & 2 & 5 \end{pmatrix}$$

One sees that when mounted together they produce the substitution

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}.$$

Permutation P is termed the product of A and B: P = A·B. The product A·B is computed from A and B as follows: Any number is transposed according to substitution A, then the result is transposed again according to B. In our example in A number 1 is replaced by 3 and in B 3 is left unchanged, i.e. P replaces 1 by 3, 2 is changed to 1 by substitution A and B changes 1 to 4, hence in the product AB 2 changes to 4, etc. Naturally it is universally true that when two wheels are mounted together the product of the pertinent substitutions is generated.

One speaks of a product in the formation of AB because certain properties hold for this calculation which are familiar from ordinary multiplication of numbers. One can, for instance, add after A and B a third wheel C with a substitution we will call C. The substitution generated by the three wheels can be calculated by regarding wheels A and B together as a new wheel F and thus getting the resultant wiring of F and C. The pertinent substitution is FC = (AB)C. But one can also take B and C together as G and then has AG = A(BC).

In both cases one has the same substitution: $A(BC) = (AB)C$. We can now shorten our expression to ABC. In like manner the products of more than three factors can be defined. The law involved in the equation $(AB)C = A(BC)$ is called the associative law. This law, namely that in multiplying one may group the factors in any order, is well known from the formation of products of ordinary numbers.

One law for the products of numbers does not hold for the multiplication of substitutions. In general AB is different from BA (this is also true in our example). Hence in our product everything depends on the sequence of the factors. Two substitutions A and B for which the equation $AB = BA$ holds good are termed commutative.

Thus far is our discussion of the wirings we have started with the contact pins and considered the connections to the flush contacts, i.e. we have so to speak been running through the cylinder in the direction from the pins to the flat contacts. We can now choose the other direction. The substitution which the cylinder with wiring W yields we will designate W^{-1}. One derives W^{-1} from W, as is readily seen, by transposing the lines and then rearranging the numbers of the new upper line in their normal sequence. One recognizes at once that

$$W\,W^{-1} = W^{-1}\,W = E = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & 25 & 26 \\ 1 & 2 & 3 & 4 & 5 & 6 & \cdots & 25 & 26 \end{pmatrix}$$

The substitution E, which converts each number into itself, is termed the <u>identity</u> substitution. Substitution W^{-1} is termed inverse to W. In our example

$$A^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 6 & 4 & 3 \end{pmatrix} \qquad \text{and } A^{-1}\,A = A\,A^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

One can readily verify the rule $(AB)^{-1} = B^{-1}\,A^{-1}$.

3. The turning of a wheel

Let wheel A be mounted between two discs S_1 and S_2 so that it can revolve. Let discs S_1 and S_2 each have a circle of 6 contacts corresponding to those of A. Let these contacts be numbered 1 - 6 in such fashion that like numbered contacts of S_1 and S_2 are opposite each other. If A is placed so that each contact pin of A touches the correspondingly numbered contact of S_1 (and consequently flush contacts of A accord in number with contacts of S_2) then the contacts of S_1 and S_2 are connected through wheel A according to the substitution of wheel A, i.e. if one interprets the upper line in

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 2 & 4 \end{pmatrix}$$

as the numbers of the contacts of S_1 and the lower line as the numbers of the contacts of S_2, then the vertical pairs represent the contacts connected with one another.

If one turns wheel A 1/6 of a complete revolution so that now contact 2 of A touches 1 of S_1 and S_2 etc., the contacts of S_1 and S_2 are now connected according to the substitution

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

As one easily figures out, $Q = Z\,A\,Z^{-1}$ where Z means the substitution $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$, i.e. that permutation where each term is replaced by the next higher and the last by 1. According to 2.,

$$Z^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

One calls Z a cyclic substitution and writes also $Z = (1\ 2\ 3\ 4\ 5\ 6)$.

The rule confirmed for our case holds good generally only that in the case of 26 contacts we write $Z = (1\ 2\ 3\ \dots\ 25\ 26)$. For if the substitution of the wheel is $\left(\frac{i}{i^*}\right)$ where $(i, i^* = 1, 2, \dots, 26)$, then in the initial position contact i of S_1 is connected with contact i* of S_2; and after 1/26 revolution contact i of S_1 is connected with $(i+1)^* - 1$ of S_2; that however means that after the motion we have the substitution $Z\binom{i}{i*} Z^{-1}$. If one turns another 1/26 of a revolution one gets the permutation $Z\,Z\binom{i}{i*} Z^{-1}Z^{-1} = Z^2 \binom{i}{i*} Z^{-2}$; in general after k turns one gets $Z^k\binom{i}{i*} Z^{-k}$ where Z^k signifies a product of k factors Z and $Z^{-k} = (Z^k)^{-1}$. It is easy to see that $Z^{26} \equiv E$.

4. The reversing wheel

A further unit of the Enigma is the so-called reversing wheel (Umkehrwalze). It is similar to the cipher wheels in construction but has only one set of contacts. These contact pins are wired up two by two through the interior of the wheel. This wheel also can be assigned a substitution by writing the numbers of the pins in the upper line and in the lower line beneath each one the number to which it is wired. If below i of the upper line we find k, obviously below k we must find i, since the two are connected. From this it follows that: if U is the substitution associated with the reversing wheel, $U = U^{-1}$, therefore $U^2 = E$.

5. The operation of the Enigma

In the Enigma there are three cipher wheels A, B, C and a reversing wheel U one alongside the other (cf. figure 3). These turn on an axle. On the disc S are 26 contacts which are connected to a keyboard like that of a typewriter and also to 26 lamps. The keys are marked with the 26 letters of the alphabet and each lamp lights to a letter on a glass plate.

If one depresses a key, say x, current enters through the corresponding contact of the end plate S into the maze of wheels. It traverses these in the order $A \rightarrow B \rightarrow C \rightarrow U \rightarrow C \rightarrow B \rightarrow A$ and comes out at some definite contact of S. The lamp wired to this contact lights up some letter, say y. Conversely if one presses key y the letter x lights up. In other words a reciprocal T_{26} (26 letter substitution alphabet) is produced.

After what has already been said it is not hard to compute the substitutions corresponding to this T_{26}, i.e. that substitution which shows how the contacts of S (end plate) are connected through the cipher wheels and reversing wheel. If A, B, C, and U stand in the basic position, i.e. so that all contacts touch like numbers, the corresponding substitution is:

$$P = A\,B\,C\,U\,C^{-1}\,B^{-1}\,A^{-1}.$$

If one wheel is advanced one step, i.e. so that contact 2 of A touches contact 1 of S and B, then according to (3) the substitution A is replaced by $Z\,A\,Z^{-1}$; similarly when other wheels move.

Now if one moves wheels A, B, and C by $\frac{k}{26}$, $\frac{l}{26}$, and $\frac{m}{26}$ of a full revolution, one gets the substitution

$$P_{k,l,m} = (Z^k A Z^{-k})(Z^l B Z^{-l})(Z^m C Z^{-m}) U (Z^m C^{-1} Z^{-m})(Z^l B^{-1} Z^{-l})(Z^k A^{-1} Z^{-k}).$$

To abbreviate we write $P_{k,l,m} = (k,l,m)$ and note that by Z^0 we understand the identity permutation E.

Thus there exists a one-to-one correspondence between the hitherto considered substitutions of the numbers 1 - 26 and the T_{26}. The association of the numbers with the letters depends on the connection of the contacts of S with the keys and lamps. In the usual commercial form of the Enigma the numbers 1, 2, ..., 25, 26 of the series are associated with the letters q w e r t z u i o a s d f g h j k p y x c v b n m l. This sequence comes from the arrangement of the keys on a typewriter. The Enigma we worked on had a like arrangement, however one could readily have determined any other.

A drive mechanism coupled with the keys of tne Enigma causes wheel A to move forward 1/26 of a revolution each time a key is depressed and wheels B and C to move in a fixed manner. Starting with $[0,0,0]$ the machine generates successively the following substitution alphabets: *

$P_1 = [0,0,0]$	$P_{651} = [0,0,1]$	$P_{1301} = [0,0,2]$	$\vdots$
$P_2 = [1,0,0]$	$P_{652} = [1,0,1]$	$\vdots$	$\vdots$
$\cdots$	$\vdots$	$\vdots$	$\vdots$
$P_{25} = [24,0,0]$	$\vdots$	$\vdots$	$\vdots$
$P_{26} = [25,1,0]$	$\vdots$	$\vdots$	$\vdots$
$P_{27} = [0,1,0]$	$P_{677} = [0,1,1]$	$\vdots$	$\vdots$
$\cdots$	$\vdots$	$\vdots$	$\vdots$
$P_{648} = [23,24,0]$	$\vdots$	$\vdots$	$\vdots$
$P_{649} = [24,24,0]$	$P_{1299} = [24,24,1]$	$\vdots$	$\vdots$
$P_{650} = [25,25,0]$	$P_{1300} = [25,25,1]$	$P_{1950} = [25,25,2]$	$\vdots$
$\vdots$	$P_{15601} = [0,0,24]$	$P_{16251} = [0,0,25]$	
$\vdots$	$P_{15602} = [1,0,24]$	$P_{16252} = [1,0,25]$	
$\vdots$	$\vdots$	$\vdots$	
$\vdots$	$P_{16249} = [24,24,24]$	$P_{16899} = [24,24,25]$	
$\vdots$	$P_{16250} = [25,25,24]$	$P_{16900} = [25,25,25]$	

These permutations repeat themselves periodically from here on, i.e. $P_{16901} = P_1$, $P_{16902} = P_2$, ...

Note: Observe that
1) wheel A causes wheel B to move between positions 24 and 25,
2) wheel B normally causes wheel C to move between 25 and 0, and
3) the motion of any wheel effects the simultaneous motion of all wheels to its left (in our scheme).

Encipherment with the Enigma proceeds by striking successively the keys corresponding to the plain text letters and copying off the corresponding cipher text letters revealed by the lamps. The first plain text letter will therefore be enciphered with the T_{26} pertaining to P_1, the second with that pertaining to P_2, etc. Since the substitutions P_n and hence the T_{26} are reciprocal, decipherment proceeds in like manner, typing the cipher text and reading off the plain text. Of course encipherment and decipherment must both be made with the same original setting.

Each of the four wheels of the Enigma has around its edge a ring with the 26 letters of the alphabet. These rings serve to establish the setting of the wheels. This setting of the machine, indicated by four letters, is termed the "outer setting." For this outer setting one has 26^4 possibilities.

These letter rings are so attached to the real cipher discs that they can be rotated. The notches in which the drive mechanism engages are firmly united with the letter rings. For the setting of the letter rings with respect to the cipher wheel proper there are also 26^4 possibilities; each such setting is likewise indicated by a group of four letters. This is known as the "inner setting."

A further possibility of variation of the machine exists in the six possible arrangements of the three wheels A, B, and C.

Finally we may point out that in the Enigma the wheels are arranged in reverse order of figure 3, i.e. the disc S (end plate) is at the right and the reversing wheel at the left. Of course what has been said holds good for this sequence. Our figure is drawn to accord as far as possible with the text.

II. Determining the wiring of an Enigma from a sequence of T_{26} (substitution alphabets)

1. Cryptanalytic foundation

There was at hand a considerable number of messages which had thoughtlessly been enciphered with the same inner and outer initial setting. Hence it was possible by superimposing the telegrams to solve the individual T_{26}'s (substitution alphabets) column by column, in doing which one could also make use of the fact that these T_{26}'s must be reciprocal. In this way one obtained a series of 50 - 150 successive T_{26}'s, some of them with gaps. For each of these sequences the outer setting was known and for part of them the inner setting was also known, as well as the wheel order in the original machine. There was also a surmise as to the wiring of the reversing wheel U which eventually proved to be correct. However, even without this guess, the wiring of U could have been figured out mathematically.

2. Theoretical calculation of the wheel wiring

To present first the principle involved in calculating the wirings A, B, C, and U, we consider as given a sufficiently long series F of successive T_{26}'s produced by the machine. The T_{26}'s or the substitutions of this sequence we designate P_1, P_2, ... without limiting generality, we can assume that P_1 is the first permutation after a simultaneous movement of wheels B and C; since our sequence F was presumed to be of adequate length, such a substitution surely occurs therein and in what follows we might examine only the portion beginning there. With the numbering of the contacts assigned in I, it was purely arbitrary which contact was assigned the number 1. Still making use of this liberty, we may further assume that $P_1 = [0,0,0]$. This brings our notation into harmony with I 5. Accordingly

$$P_1 = A(BCUC^{-1}B^{-1})A^{-1}$$
$$P_2 = ZAZ^{-1}(BCUC^{-1}B^{-1})ZA^{-1}Z^{-1} .$$

One sees that the central term in parenthesis is the same in both equations, which is clear since in passing from P_1 to P_2 only wheel A advanced one step. The fact that in passing from P_1 to P_2 only wheel A is involved (and this in a known manner), makes it comprehensible that one can deduce from P_1 and P_2 together certain properties of wheel A. It appears that by adding a few more pairs of successive substitutions it is even possible to calculate A almost completely. Once A is known, one can form from P a new sequence G which is no longer dependent in any way on A, viz.:

$$Q_1 = A^{-1}P_1A = B(CUC^{-1})B^{-1}$$
$$Q_{27} = A^{-1}P_{27}A = ZBZ^{-1}(CUC^{-1})ZB^{-1}Z^{-1}$$
$$Q_{651} = A^{-1}P_{651}A = B(ZCZ^{-1}UZC^{-1}Z^{-1})B^{-1}$$
$$Q_{677} = A^{-1}P_{677}A = ZBZ^{-1}(ZCZ^{-1}UZC^{-1}Z^{-1})ZB^{-1}Z^{-1}$$

....

This sequence can be used in corresponding fashion to calculate B. Using a third sequence, which is not dependent on B, C is figured, and finally U.

Carrying out these calculations in detail calls for a certain amount of practice in using the symbols here introduced. Moreover, since too full a description would make it difficult to take in quickly, we will assume down to the end of this section 2 some familiarity with substitutions and express ourselves somewhat more briefly in presenting our calculations.

With $X = AZA^{-1}Z^{-1}$ we get $X^{-1}P_1X = P_2$.
With this equation X is determined except for a lefthand factor which is commutative with P_1; i.e., if

$\bar{X}^{-1}P_1\bar{X} = P_2$ and one assumes $\bar{X} = KX$ then

$\bar{X}^{-1}P_1\bar{X} = X^{-1}K^{-1}P_1KX = X^{-1}P_1X$, therefore $K^{-1}P_1K = P_1$,

i.e., $KP_1 = P_1K$. Likewise we have the equation

$X^{-1}P_{27}X = P_{28}$.

By this equation X is determined except for a lefthand factor which is commutative with P_{27}. The two equations $X^{-1}P_1X = P_2$ and $X^{-1}P_{27}X = P_{28}$ determine X except for a lefthand factor which is commutative with both P_1 and P_{27}. Now if there is a set M of substitutions, P_m with $m = 26n - 1$, such that the identity is the only substitution commutative with all P_m, then by the equation

$$X^{-1}P_mX = P_{m+1},$$

where P_m runs through all the substitutions of M, X is uniquely determined.

This case has occurred in all examples which have actually come up. The set M consisted of from three to five substitutions.

If X is determined one gets from $X = AZA^{-1}Z^{-1}$

$$XZ = AZA^{-1}.$$

This equation determines A except for a power of Z as a righthand factor, since a cycle is commutative only with its powers.

A cannot be determined more exactly by sequence F alone, for with every choice of A among the 26 possibilities B, C, and U can be so determined as to generate sequence F. That A cannot be thus determined uniquely is clear; conceive of the wheels as constructed of pliable material, then one could, for example, twist the two sides of wheel A with respect to one another; a like twisting of wheel B would compensate for this, however. Such a twisting would exactly correspond to the replacement of A by AZ^p.

For the following we select as A one solution from among those possible for $XZ = AZA^{-1}$. From sequence F we now form the sequence G mentioned in the beginning: Q_1, Q_{27}, Q_{651}, Q_{677} .... . From the pairs Q_1, Q_{27}; Q_{651}, Q_{677}; .... we derive first $Y = BZB^{-1}Z^{-1}$. From this we get B; what was said about the non-uniqueness of the solution for A holds for B.

To determine C we cannot proceed in exactly analogous fashion. We form the sequence

$$R_1 = B^{-1}Q_1B = CUC^{-1}$$
$$R_{651} = B^{-1}Q_{651}B = ZCZ^{-1}UZC^{-1}Z^{-1}$$
$$R_{1301} = B^{-1}Q_{1301}B = Z^2CZ^{-2}UZ^2C^{-1}Z^{-2}$$

As one readily calculates, with $V = CZC^{-1}Z^{-1}$

$$V^{-1}R_1V = R_{651}$$
$$V^{-1}(Z^{-1}R_{651}Z)V = Z^{-1}R_{1301}Z$$
$$V^{-1}(Z^{-2}R_{1301}Z^2)V = Z^{-2}R_{1951}Z^2$$

From these equations one can determine V and from that C.

Finally U can be determined, e.g. from R_1: $U = C^{-1}R_1C$.

The method employed here to determine C can also be used to determine A and B. Carrying this out by this method calls for more computation but one can succeed with fewer members of a sequence, which in practical application is a great advantage.

3. Practical calculation of the wheel wirings.

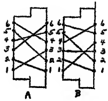
As already mentioned, our sequences of T_{26}'s contained only some 50 terms. Consequently by the method given in 2. one could at most determine the two wheels at the left (cf. Fig. 3), i.e. A and B, and to get B it was necessary to use the method described at the end of 2. But the sequences anticipated did not all correspond to wheel order A, B, C, but also to some others; if, for instance, the order C B A is found, one can easily obtain the wiring of C from one sequence belonging to this wheel order.

After tne wirings of A, B, C, and U had been determined, came the furtner problem of studying the skipping motion of tne wheels in detail. The question calling for an answer was: at what position of A does B move one step? This cannot be determined from our previous theoretical considerations since we have arbitrarily considered a substitution immediately after the simultaneous movement of all three wheels (0,0,0). The considerations which finally led to solution of this problem were in part rather complex and it would lead too far afield to reproduce them here. Essential was the fact that we knew the outer settings corresponding to our sequences. Use was also made of the fact that the original wiring of U was known or at least suspected.

In this stage of the work an Enigma with the recovered wirings and the recovered drive-mechanism was constructed with which all messages received were readily read.

This machine probably did not agree fully with the original for the wirings had not been uniquely determined by the sequences. In order to assure current reading of traffic even when the inner setting was changed (the outer setting was supplied by an indicator), it seemed desirable to see how our machine differed from the original. This was solved very quickly, because for setting the original a pronouncable four letter word was always chosen.

FIG. 1



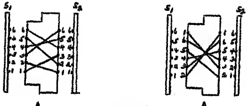


FIG. 2

FIG 3